In re Patent Application of:
SONZOGNI ET AL.
Serial No. **09/914,315**
Filing Date: **AUGUST 24, 2001**
_____/

In the Claims:

Claims 1-4 (Previously Cancelled).

5. (Previously Added) A chip card comprising:

a microprocessor including an operating system working with a set of instructions, said microprocessor comprising a first register for storing a first code, on at least one check bit, for an entity to be executed, said first register being updated based upon a call instruction and a return instruction during execution of a new entity;

a memory connected to said microprocessor for storing a plurality of application programs; and

a checking device connected to said microprocessor for checking, as a function of the at least one check bit, whether access to locations in said memory is authorized for the new entity.

6. (Previously Added) A chip card according to Claim 5, wherein said microprocessor comprises a second register for storing a second code for the application programs active when a last call instruction was sent.

7. (Previously Added) A chip card according to Claim 6, wherein said second register can not be directly accessed.

8. (Previously Added) A chip card according to Claim 5, wherein each entity is one of the plurality of application programs.

9. (Previously Added) A chip card according to Claim

5, wherein each entity causes a hardware event.

10. (Previously Added) A chip card according to Claim 9, wherein the hardware event resets said microprocessor.

11. (Previously Added) A chip card according to Claim 5, wherein said first register is updated in response to the return instruction.

12. (Previously Added) A chip card according to Claim 5, wherein said checking device provides a control signal to said microprocessor for providing access to the locations of said memory if the new entity is authorized.

13. (Previously Added) A chip card according to Claim 5, wherein said checking device compares the address locations to be accessed in said memory and the first code in said first register.

14. (Previously Added) A chip card comprising:
a microprocessor comprising
a first register for storing a first code, on at least one check bit, for an application program to be executed, said first register being updated based upon a call instruction and a return instruction during execution of a new application program, and
a second register for storing a second code for an application program active when a last call

instruction was sent;

a memory connected to said microprocessor for storing the application program; and

a checking device connected to said microprocessor for checking, as a function of the at least one check bit, whether access to locations in said memory is authorized for the new application program, said checking device providing a control signal to said microprocessor for providing access to the locations of said memory if the new application program is authorized.

15. (Previously Added) A chip card according to Claim 14, wherein said second register can not be directly accessed.

16. (Previously Added) A chip card according to Claim 14, wherein each application program causes a hardware event.

17. (Currently Amended) A chip card according to Claim 16, wherein the hardware event ~~causes~~ resets said microprocessor.

18. (Previously Added) A chip card according to Claim 14, wherein said first register is automatically updated in response to the return instruction.

19. (Previously Added) A chip card according to Claim 14, wherein said checking device compares the address locations to be accessed in said memory and the first code in

said first register.

20. (Previously Added) A method for securing access to a chip card comprising a microprocessor including an operating system working with a set of instructions, and a memory connected to the microprocessor for storing a plurality of application programs, the method comprising:

storing a first code, on at least one check bit, in a first register of the microprocessor for an entity to be executed;

updating the first register based upon a call instruction and a return instruction during execution of a new entity; and

checking, as a function of the at least one check bit, whether access to locations in the memory is authorized for the new entity.

21. (Previously Added) A method according to Claim 20, further comprising storing a second code in a second register of the microprocessor for an application program active when a last call instruction was sent.

22. (Previously Added) A method according to Claim 21, wherein the second register can not be directly accessed.

23. (Previously Added) A method according to Claim 20, wherein each entity is one of the plurality of application programs.

24. (Previously Added) A method according to Claim

20, wherein each entity causes a hardware event.

25. (Previously Added) A method according to Claim 24, wherein the hardware event resets the microprocessor.

26. (Previously Added) A method according to Claim 20, wherein the first register is updated in response to the return instruction.

27. (Previously Added) A method according to Claim 20, wherein checking comprises providing a control signal to the microprocessor for providing access to the locations of the memory if the new entity is authorized.

28. (Previously Added) A method according to Claim 20, wherein checking comprises comparing the address locations to be accessed in the memory and the first code in the first register.

29. (Previously Added) A method for securing access to a chip card comprising a microprocessor and a memory connected thereto for storing a plurality of application programs, the method comprising:

storing a first code, on at least one check bit, in a first register of the microprocessor for an application program to be executed;

updating the first register based upon a call instruction and a return instruction during execution of a new application program; and

checking, as a function of the at least one check

bit, whether access to locations in the memory is authorized for the new application program.

30. (Previously Added) A method according to Claim 29, further comprising storing a second code in a second register of the microprocessor for an application program active when a last call instruction was sent.

31. (Previously Added) A method according to Claim 29, wherein the second register can not be directly accessed.

32. (Previously Added) A method according to Claim 29, wherein each application program causes a hardware event.

33. (Currently Amended) A method according to ~~Claim 33~~ Claim 32, wherein the hardware event resets the microprocessor.

34. (Previously Added) A method according to Claim 29, wherein the first register is updated in response to the return instruction.

35. (Previously Added) A method according to Claim 29, wherein checking comprises providing a control signal to the microprocessor for providing access to the locations of the memory if the new application program is authorized.

36. (Previously Added) A method according to Claim 29, wherein checking comprises comparing the address locations

to be accessed in the memory and the first code in the first register.

37. (New) A chip card comprising:

a microprocessor;

a memory connected to said microprocessor for storing a plurality of application programs;

said microprocessor comprising a first register for storing a first code, on at least one check bit, corresponding to a first application program to be executed from said plurality of application programs;

if execution of said first application program requires intervention of a second application program from said plurality of application programs, then said first application program sends a call instruction to said microprocessor requesting such intervention;

said first register being updated based upon the call instruction for storing a second code, on the at least one check bit, corresponding to said second application program to be executed; and

a checking device connected to said microprocessor for checking the second code as to whether access to locations in said memory are authorized for said second application program.

38. (New) A chip card according to Claim 37, wherein said microprocessor comprises a second register for storing the first code corresponding to said first application program while said second application program is being executed; said first register also being updated based upon the first code.

39. (New) A chip card according to Claim 38, wherein after said microprocessor executes said second application program, said first register enables said microprocessor to return to said first application program.

40. (New) A chip card according to Claim 38, wherein said second register can not be directly accessed.

41. (New) A chip card according to Claim 37, wherein said first and second application programs are written in a standardized language.

42. (New) A chip card according to Claim 41, wherein said first and second application programs are loaded into said memory after the chip card has been fabricated.

43. (New) A chip card according to Claim 37, wherein said checking device provides a control signal to said microprocessor for providing access to the locations of said memory if said second application program is authorized.

44. (New) A chip card according to Claim 37, wherein said checking device compares the address locations to be accessed in said memory with the second code in said first register.